This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

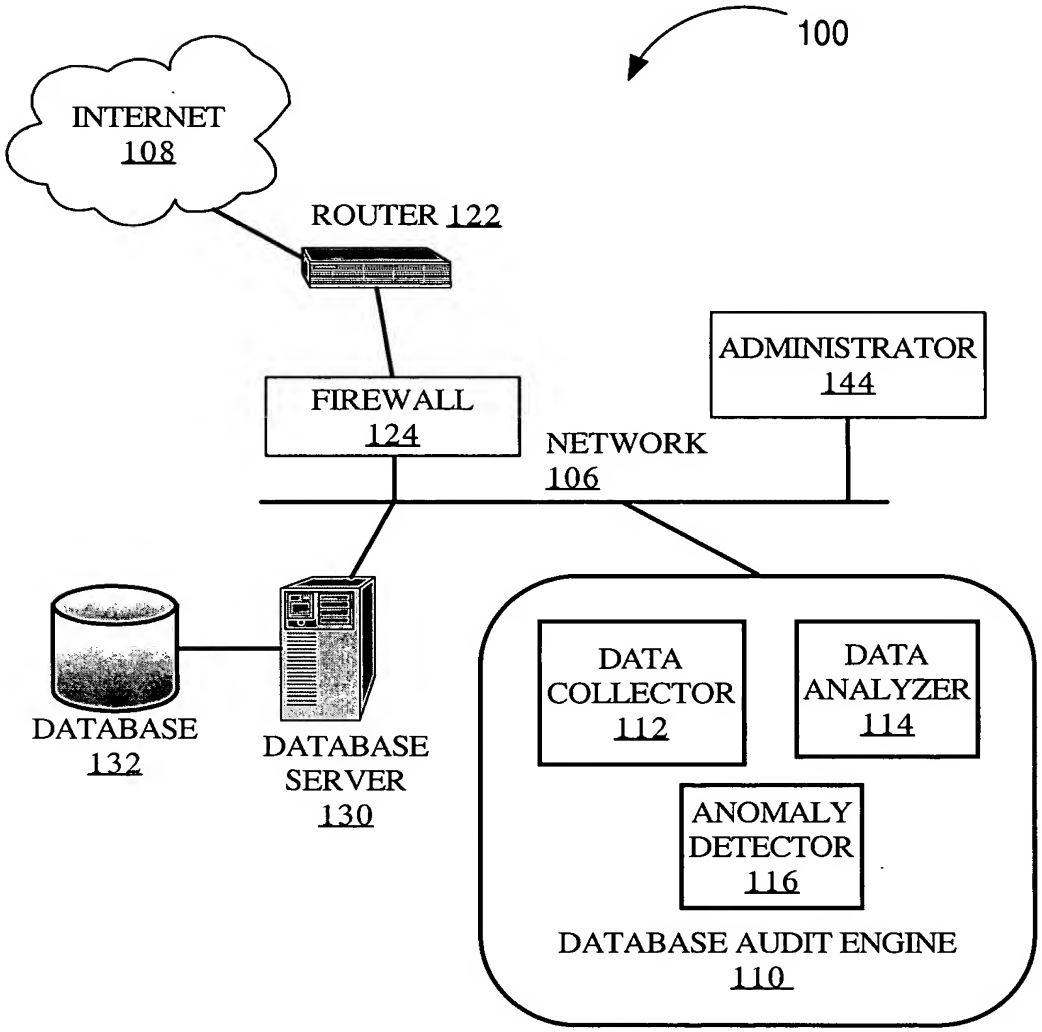
100
INTERNET
108
ROUTER 122
FIREWALL
124
ADMINISTRATOR
144
NETWORK
106
DATABASE
132
DATABASE
SERVER
130
DATA
COLLECTOR
112
DATA
ANALYZER
114
ANOMALY
DETECTOR
116
DATABASE AUDIT ENGINE
110

FIG. 1

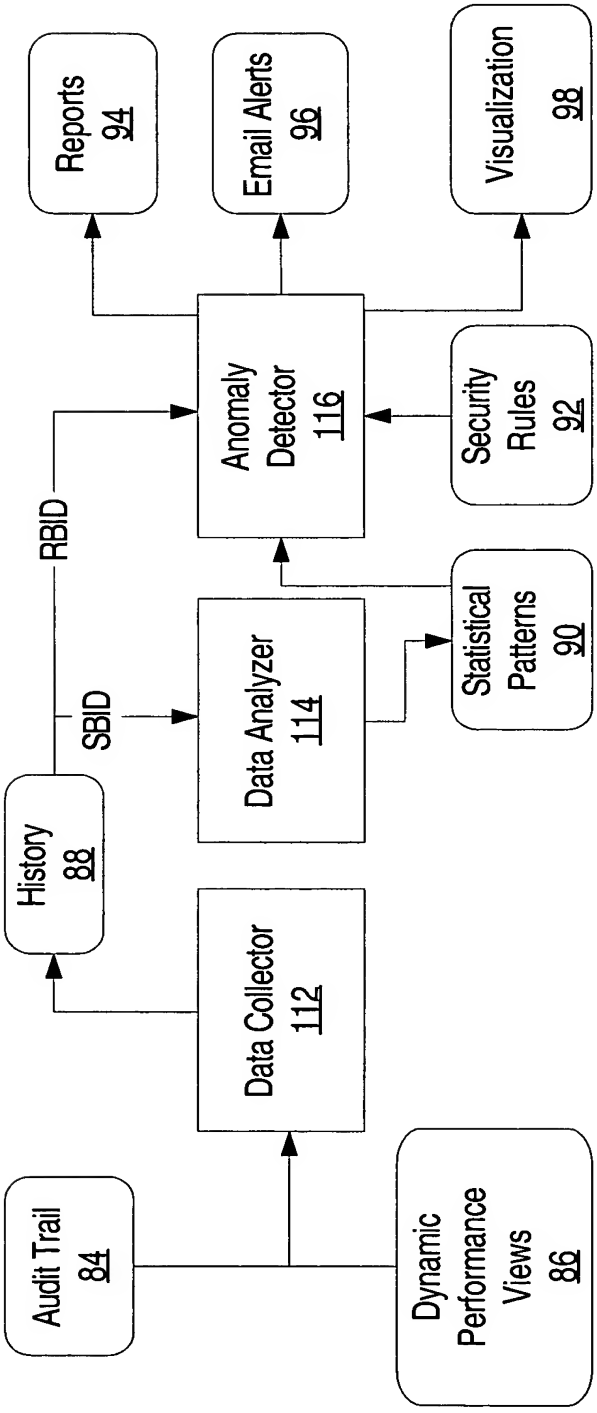
Reports 94
Email Alerts 96
Visualization 98
Anomaly Detector 116
Security Rules 92
RBID
SBID
Data Analyzer 114
Statistical Patterns 90
History 88
Data Collector 112
Audit Trail 84
Dynamic Performance Views 86

FIG. 2

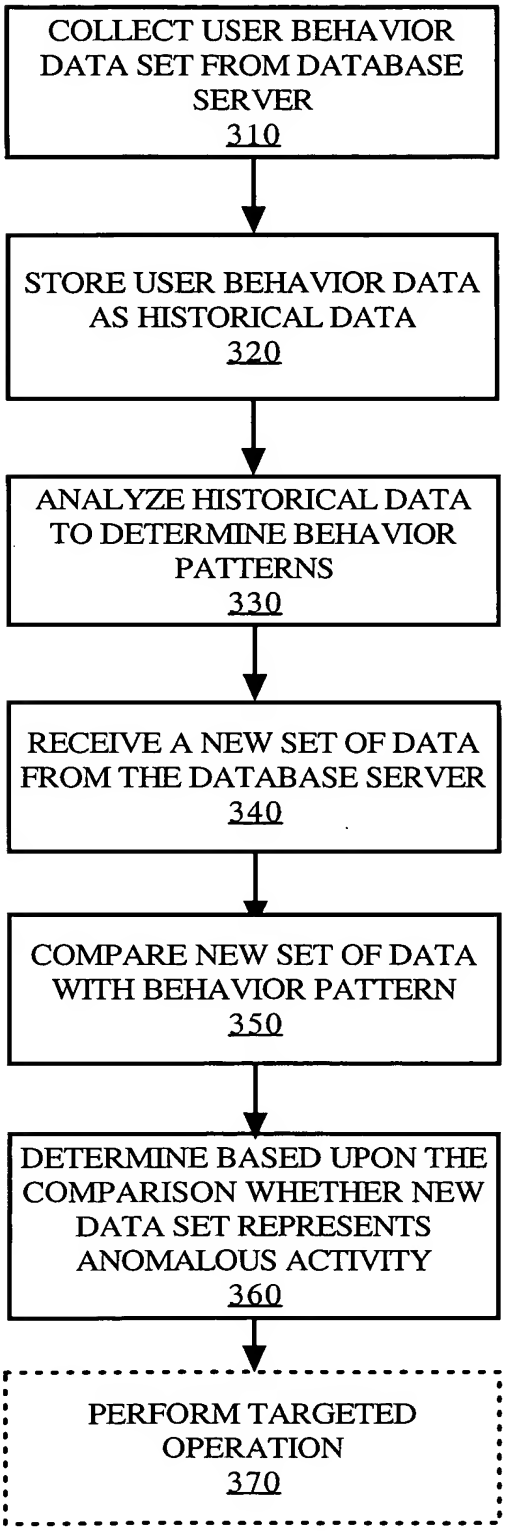
COLLECT USER BEHAVIOR DATA SET FROM DATABASE SERVER
310
STORE USER BEHAVIOR DATA AS HISTORICAL DATA
320
ANALYZE HISTORICAL DATA TO DETERMINE BEHAVIOR PATTERNS
330
RECEIVE A NEW SET OF DATA FROM THE DATABASE SERVER
340
COMPARE NEW SET OF DATA WITH BEHAVIOR PATTERN
350
DETERMINE BASED UPON THE COMPARISON WHETHER NEW DATA SET REPRESENTS ANOMALOUS ACTIVITY
360
PERFORM TARGETED OPERATION
370

FIG. 3A

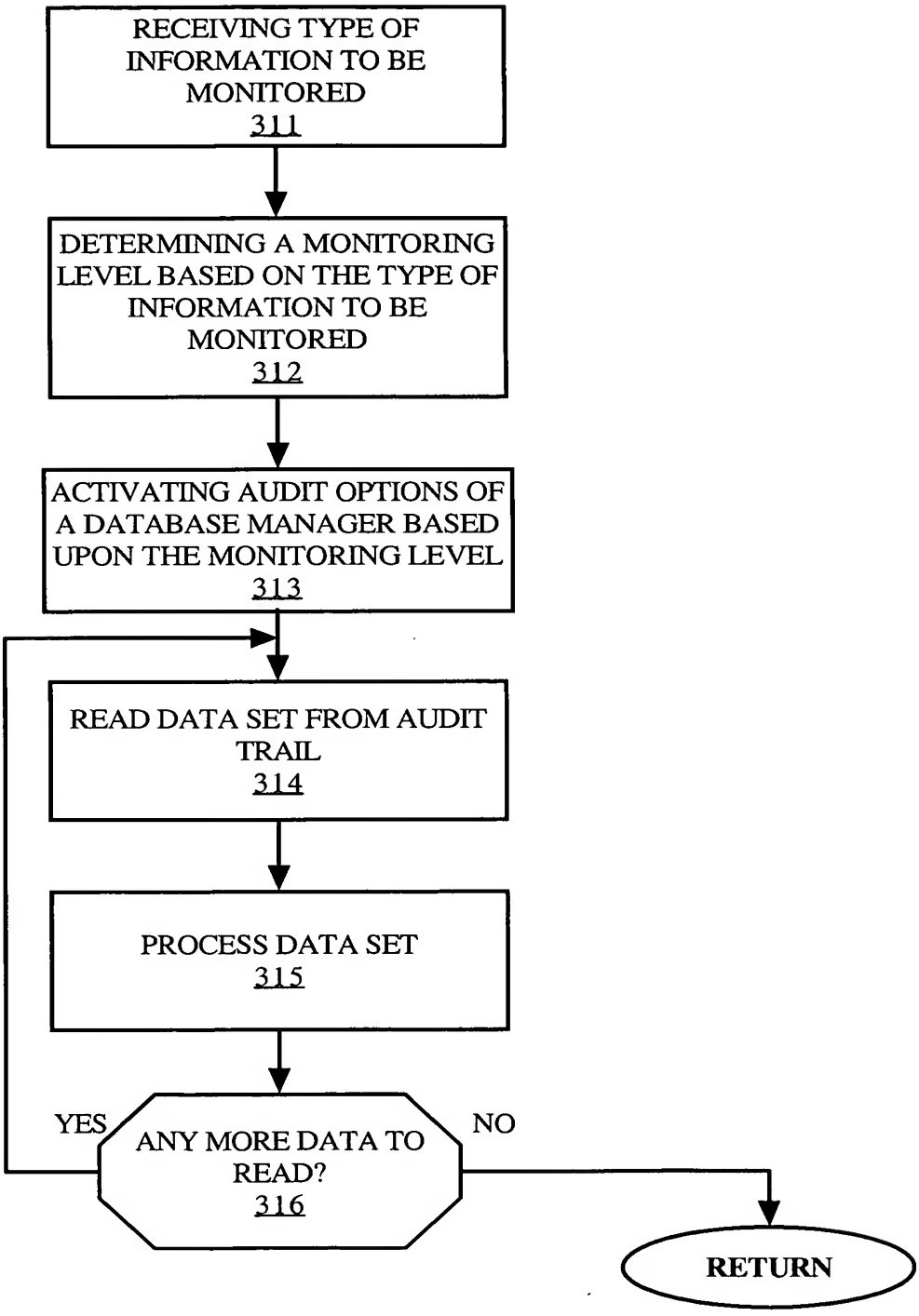
RECEIVING TYPE OF INFORMATION TO BE MONITORED
311
DETERMINING A MONITORING LEVEL BASED ON THE TYPE OF INFORMATION TO BE MONITORED
312
ACTIVATING AUDIT OPTIONS OF A DATABASE MANAGER BASED UPON THE MONITORING LEVEL
313
READ DATA SET FROM AUDIT TRAIL
314
PROCESS DATA SET
315
YES
ANY MORE DATA TO READ?
316
NO
RETURN

FIG. 3B

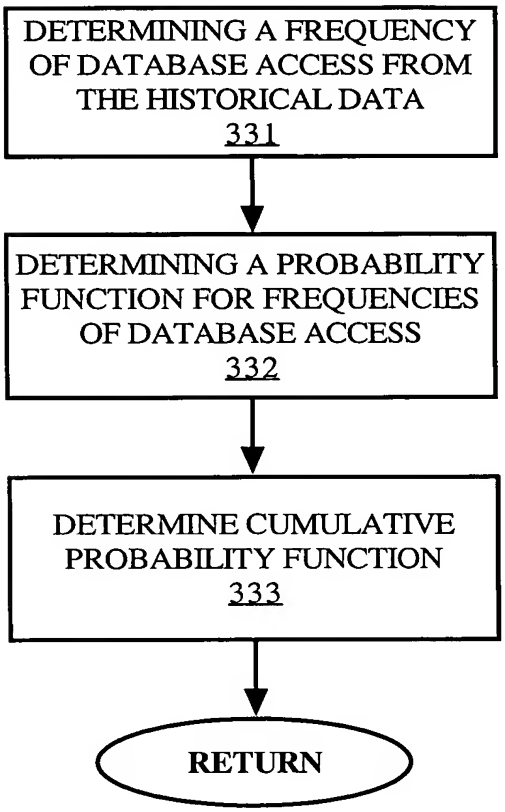
DETERMINING A FREQUENCY OF DATABASE ACCESS FROM THE HISTORICAL DATA
331
DETERMINING A PROBABILITY FUNCTION FOR FREQUENCIES OF DATABASE ACCESS
332
DETERMINE CUMULATIVE PROBABILITY FUNCTION
333
RETURN

FIG. 3C

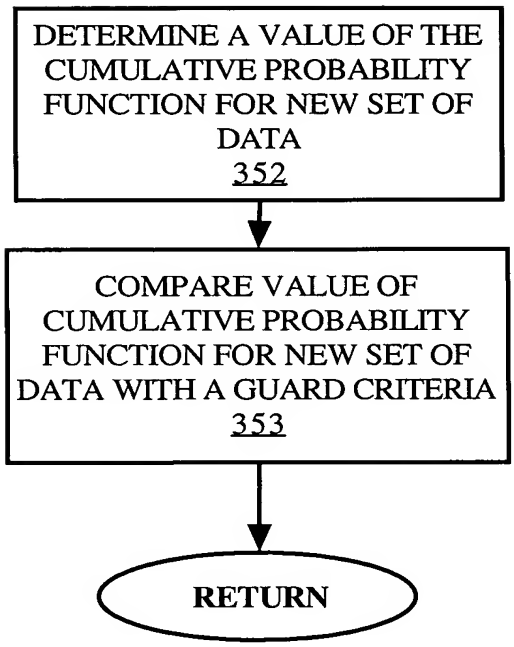
DETERMINE A VALUE OF THE CUMULATIVE PROBABILITY FUNCTION FOR NEW SET OF DATA
352
COMPARE VALUE OF CUMULATIVE PROBABILITY FUNCTION FOR NEW SET OF DATA WITH A GUARD CRITERIA
353
RETURN

FIG. 3D

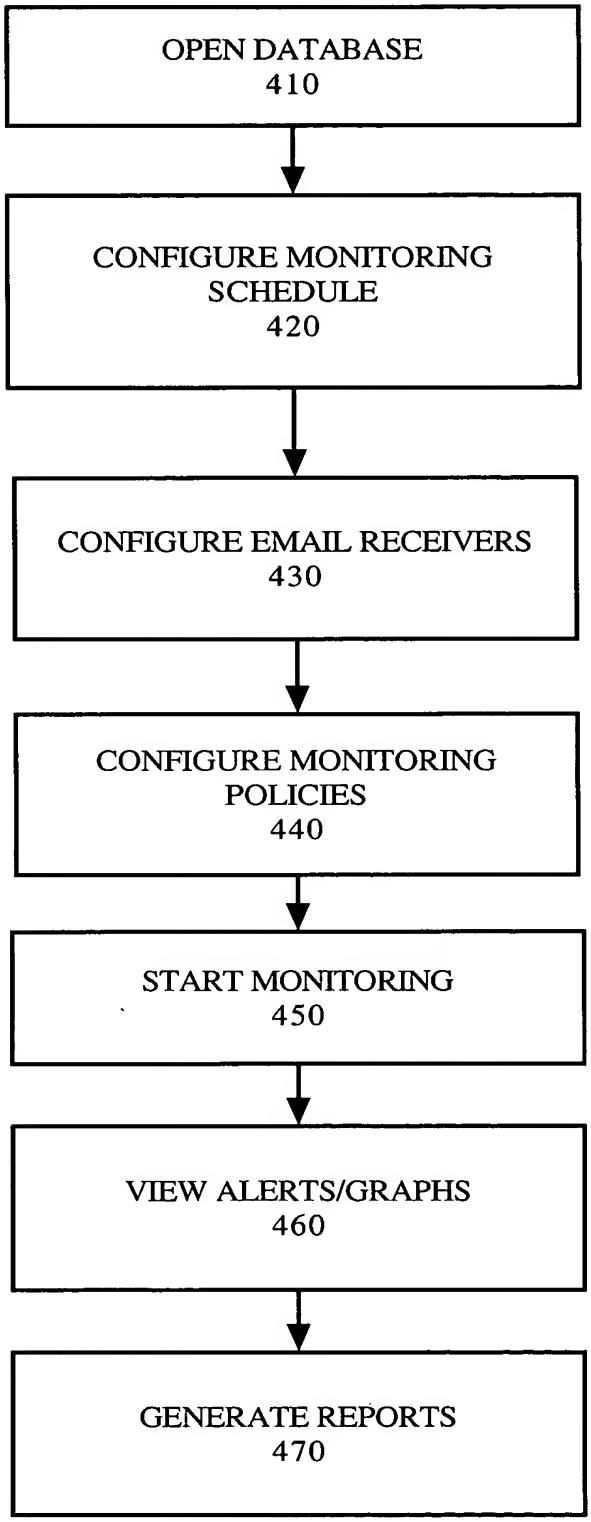
OPEN DATABASE
410
CONFIGURE MONITORING SCHEDULE
420
CONFIGURE EMAIL RECEIVERS
430
CONFIGURE MONITORING POLICIES
440
START MONITORING
450
VIEW ALERTS/GRAPHS
460
GENERATE REPORTS
470

FIG. 3E

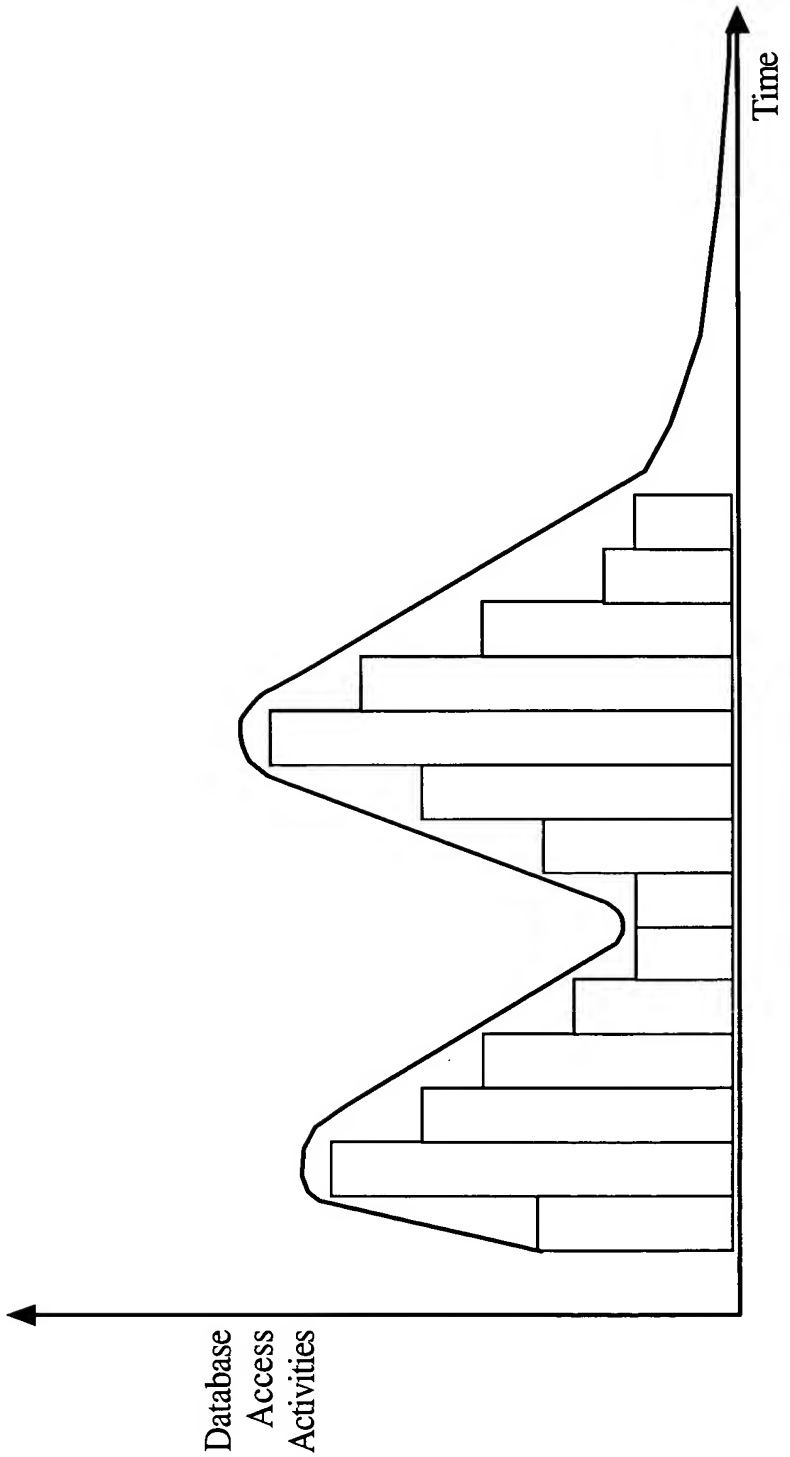

FIG. 4

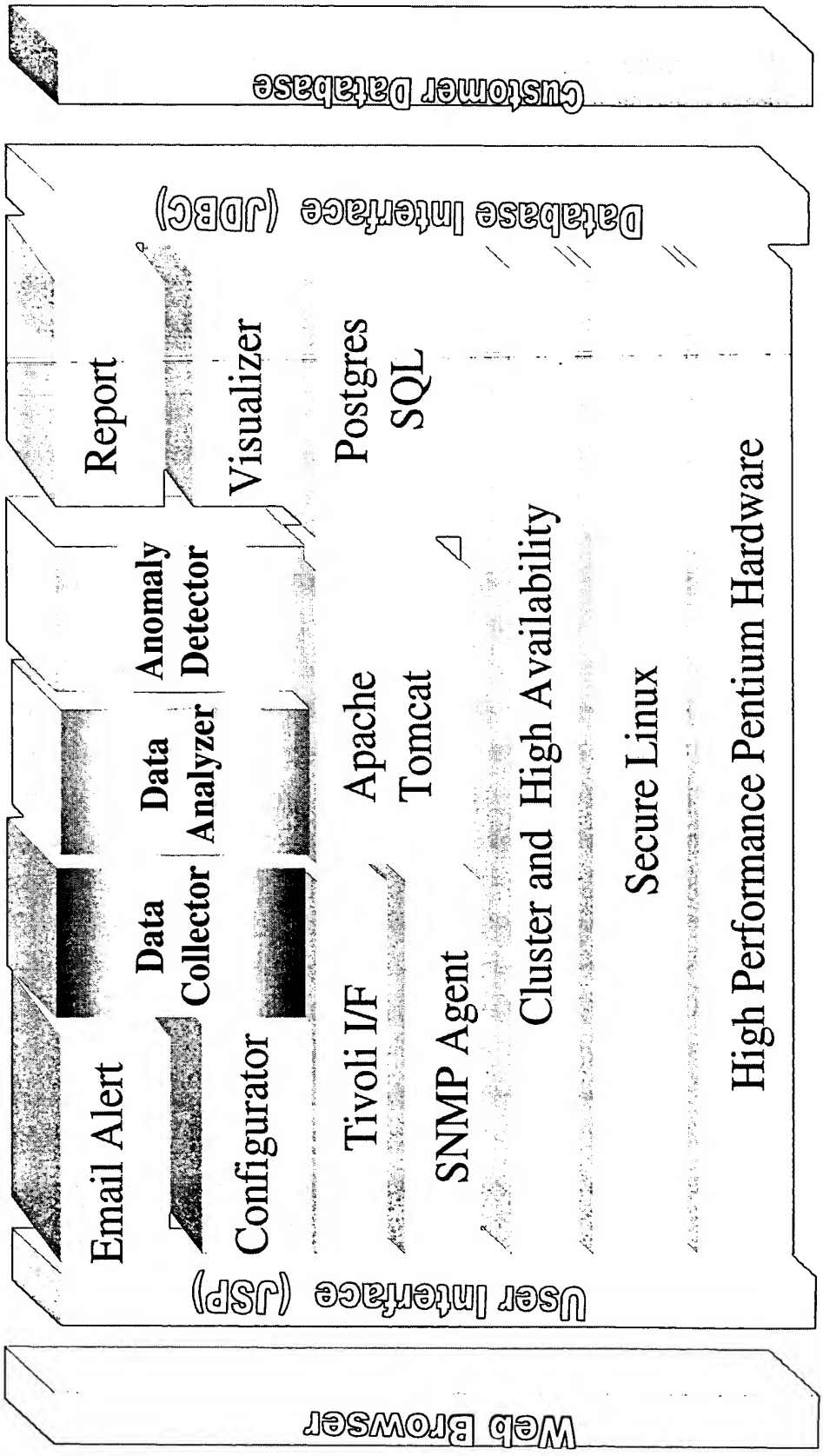
Web Browser
User Interface (JSP)
Email Alert
Configurator
Data Collector
Data Analyzer
Anomaly Detector
Report
Visualizer
Tivoli I/F
SNMP Agent
Apache
Tomcat
Postgres SQL
Cluster and High Availability
Secure Linux
High Performance Pentium Hardware
Database Interface (JDBC)
Customer Database

FIG 5

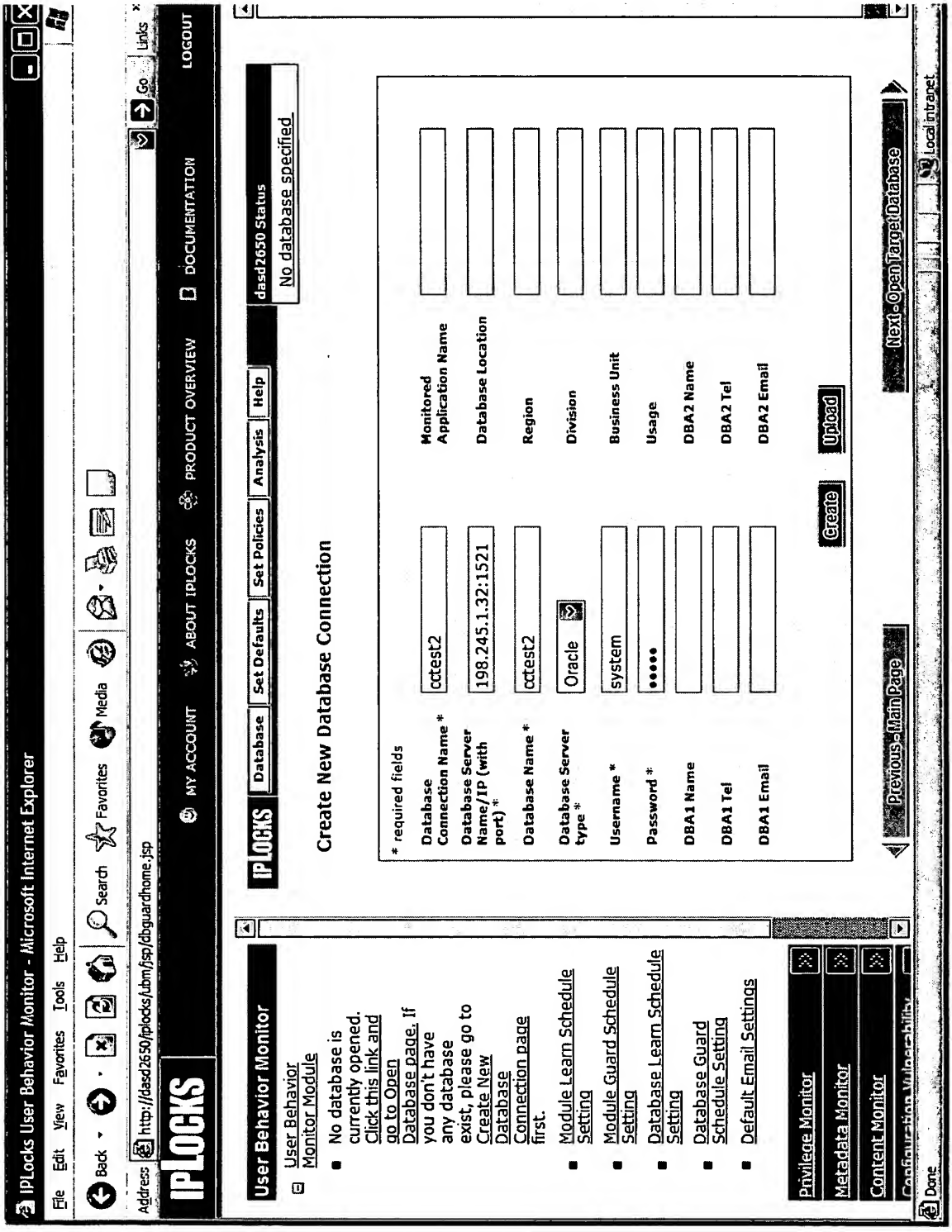
IPLocks User Behavior Monitor - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://dasd2650/iplocks/ubm/jsp/dbguardhome.jsp
IPLOCKS
MY ACCOUNT
ABOUT IPLOCKS
PRODUCT OVERVIEW
DOCUMENTATION
LOGOUT
User Behavior Monitor
User Behavior Monitor Module
No database is currently opened. Click this link and go to Open Database page. If you don't have any database exist, please go to Create New Database Connection page first.
Module Learn Schedule Setting
Module Guard Schedule Setting
Database Learn Schedule Setting
Database Guard Schedule Setting
Default Email Settings
Privilege Monitor
Metadata Monitor
Content Monitor
IPLOCKS
Database
Set Defaults
Set Policies
Analysis
Help
dasd2650 Status
No database specified
Create New Database Connection
* required fields
Database Connection Name *
cctest2
Monitored Application Name
Database Server Name/IP (with port) *
198.245.1.32:1521
Database Location
Database Name *
cctest2
Region
Database Server type *
Oracle
Division
Username *
system
Business Unit
Password *
Usage
DBA1 Name
DBA2 Name
DBA1 Tel
DBA2 Tel
DBA1 Email
DBA2 Email
Create
Upload
Previous - Main Page
Next - Open Target Database
Done
Local intranet

FIG 6A

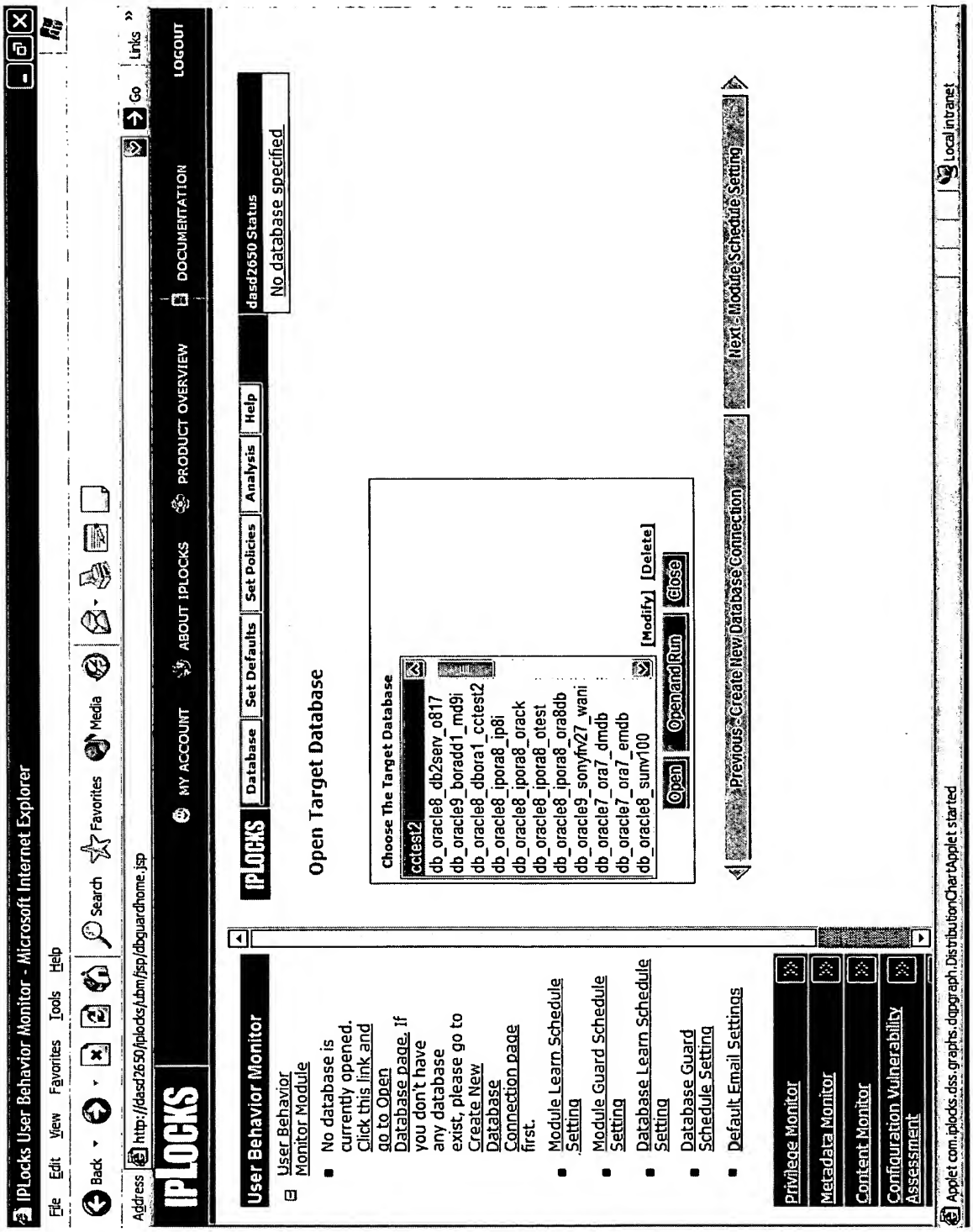
IPLocks User Behavior Monitor - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://dasd2650/iplocks/ubm/jsp/dbguardhome.jsp
Links
IPLOCKS
MY ACCOUNT
ABOUT IPLOCKS
PRODUCT OVERVIEW
DOCUMENTATION
LOGOUT
User Behavior Monitor
User Behavior Monitor Module
No database is currently opened. Click this link and go to Open Database page. If you don't have any database exist, please go to Create New Database Connection page first.
Module Learn Schedule Setting
Module Guard Schedule Setting
Database Learn Schedule Setting
Database Guard Schedule Setting
Default Email Settings
Privilege Monitor
Metadata Monitor
Content Monitor
Configuration Vulnerability Assessment
IPLOCKS
Database
Set Defaults
Set Policies
Analysis
Help
dasd2650 Status
No database specified
Open Target Database
Choose The Target Database
cctest2
db_oracle8_db2serv_o817
db_oracle9_boradd1_md9i
db_oracle8_dbora1_cctest2
db_oracle8_ipora8_ip8i
db_oracle8_ipora8_orack
db_oracle8_ipora8_otest
db_oracle8_ipora8_ora8db
db_oracle9_sonyfrv27_wani
db_oracle7_ora7_dmdb
db_oracle7_ora7_emdb
db_oracle8_sunv100
[Modify] [Delete]
Open
Open and Run
Close
Previous - Create New Database Connection
Next - Module Schedule Setting
Applet com.iplocks.dss.graphs.dqpgraph.DistributionChartApplet started
Local intranet

FIG 6B

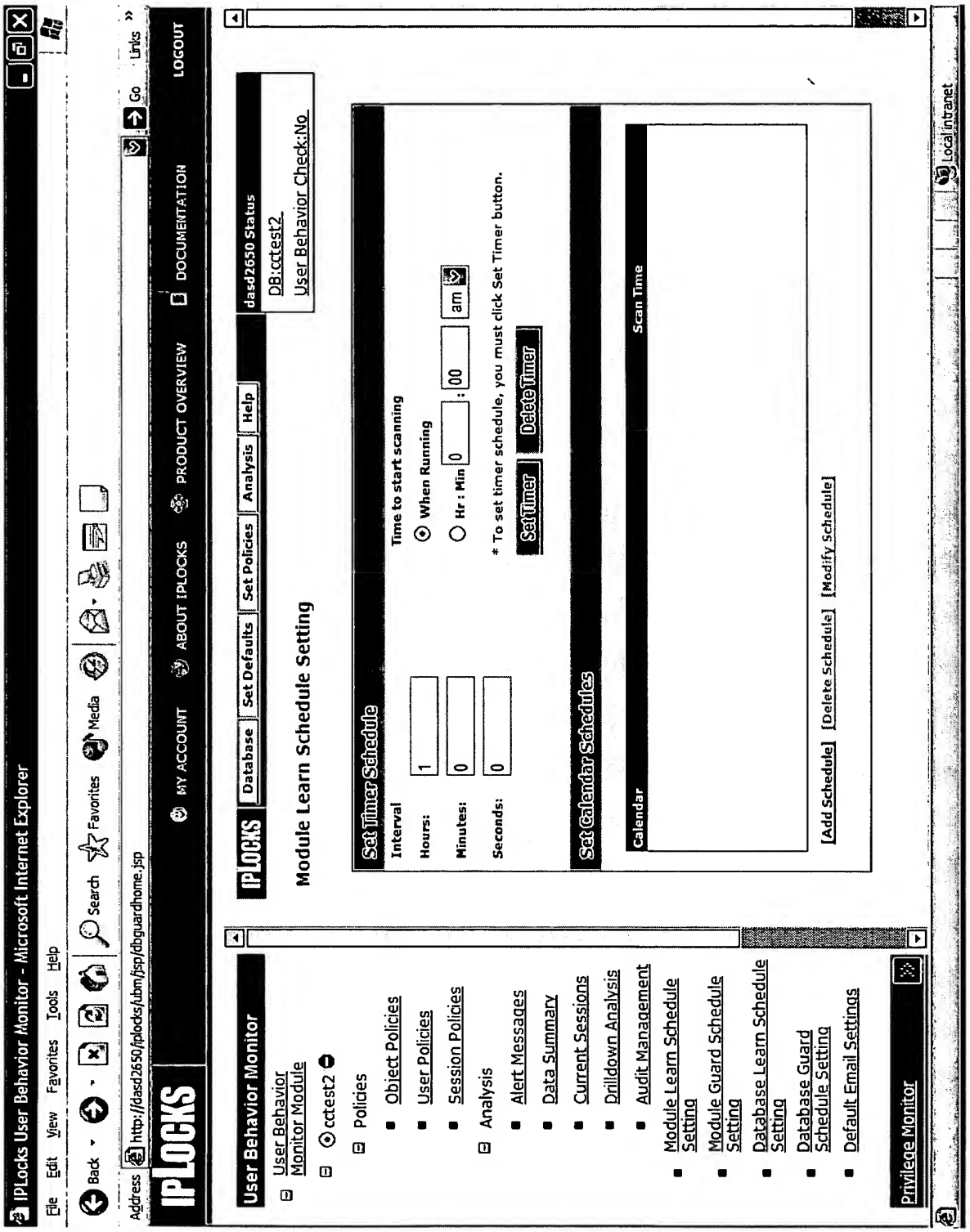
IPLocks User Behavior Monitor - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://dasd2650/iplocks/ubm/jsp/dbguardhome.jsp
Go Links
IPLOCKS
MY ACCOUNT
ABOUT IPLOCKS
PRODUCT OVERVIEW
DOCUMENTATION
LOGOUT
User Behavior Monitor
User Behavior Monitor Module
cctest2
Policies
Object Policies
User Policies
Session Policies
Analysis
Alert Messages
Data Summary
Current Sessions
Drilldown Analysis
Audit Management
Module Learn Schedule Setting
Module Guard Schedule Setting
Database Learn Schedule Setting
Database Guard Schedule Setting
Default Email Settings
Privilege Monitor
IPLOCKS
Database
Set Defaults
Set Policies
Analysis
Help
dasd2650 Status
DB:cctest2
User Behavior Check:No
Module Learn Schedule Setting
Set Timer Schedule
Interval
Hours: 1
Minutes: 0
Seconds: 0
Time to start scanning
When Running
Hr : Min 0 : 00 am
* To set timer schedule, you must click Set Timer button.
SetTimer
DeleteTimer
Set Calendar Schedules
Calendar
Scan Time
[Add Schedule] [Delete Schedule] [Modify Schedule]
Local intranet

FIG 6C

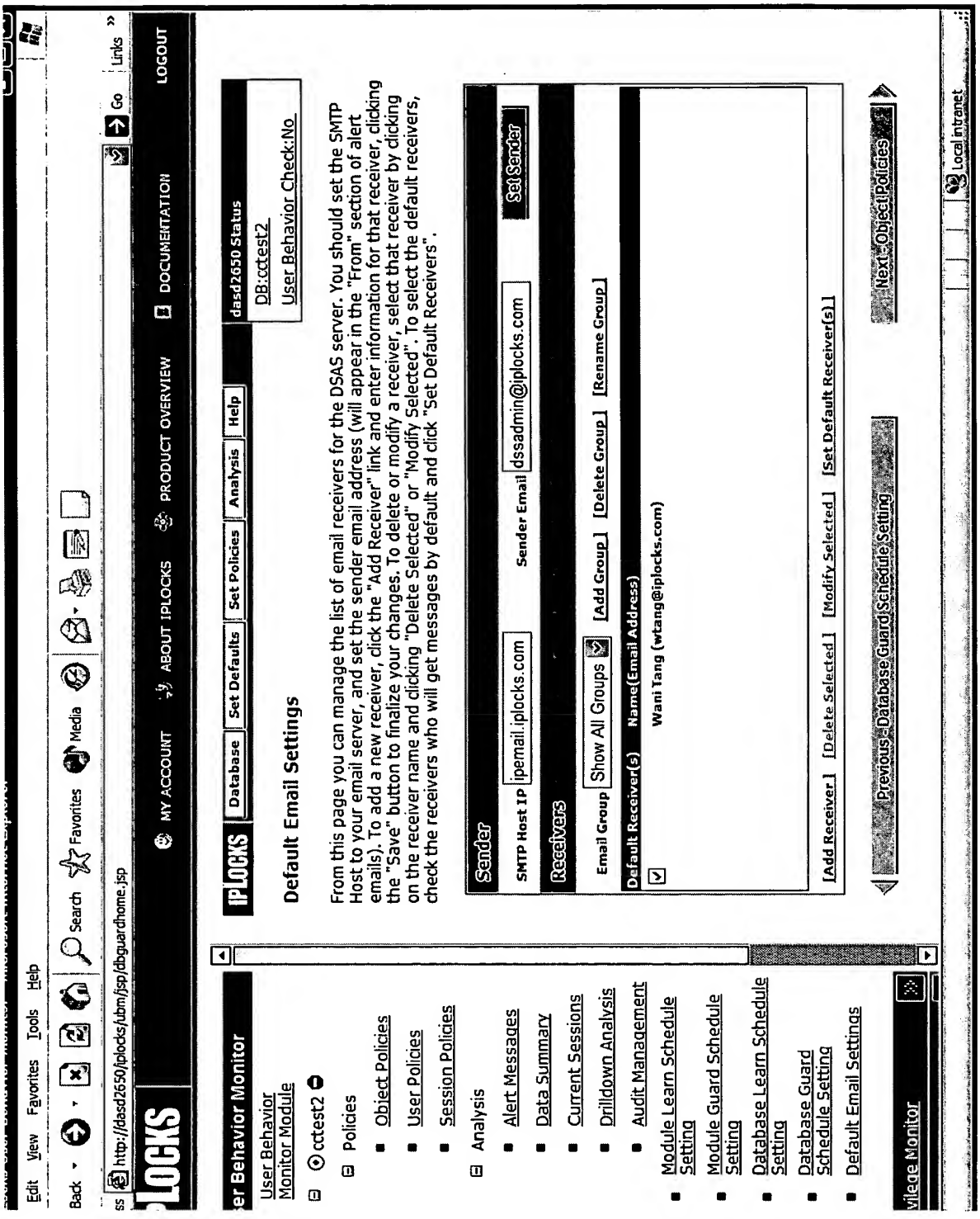
Edit View Favorites Tools Help
Back Search Favorites Media
http://dasd2650/iplocks/jdm/jsp/dbguardhome.jsp
Go Links
IPLOCKS
MY ACCOUNT ABOUT IPLOCKS PRODUCT OVERVIEW DOCUMENTATION LOGOUT
er Behavior Monitor
User Behavior Monitor Module
cctest2
Policies
Object Policies
User Policies
Session Policies
Analysis
Alert Messages
Data Summary
Current Sessions
Drilldown Analysis
Audit Management
Module Learn Schedule Setting
Module Guard Schedule Setting
Database Learn Schedule Setting
Database Guard Schedule Setting
Default Email Settings
vilege Monitor
IPLOCKS Database Set Defaults Set Policies Analysis Help
dasd2650 Status
DB:cctest2
User Behavior Check:No
Default Email Settings
From this page you can manage the list of email receivers for the DSAS server. You should set the SMTP Host to your email server, and set the sender email address (will appear in the "From" section of alert emails). To add a new receiver, click the "Add Receiver" link and enter information for that receiver, clicking the "Save" button to finalize your changes. To delete or modify a receiver, select that receiver by clicking on the receiver name and clicking "Delete Selected" or "Modify Selected". To select the default receivers, check the receivers who will get messages by default and click "Set Default Receivers".
Sender
SMTP Host IP ipemail.iplocks.com Sender Email dssadmin@iplocks.com Set Sender
Receivers
Email Group Show All Groups [Add Group] [Delete Group] [Rename Group]
Default Receiver(s) Name(Email Address)
Wani Tang (wtang@iplocks.com)
[Add Receiver] [Delete Selected] [Modify Selected] [Set Default Receiver(s)]
Previous Database Guard Schedule Setting
Next Object Policies
Local intranet

FIG 6D

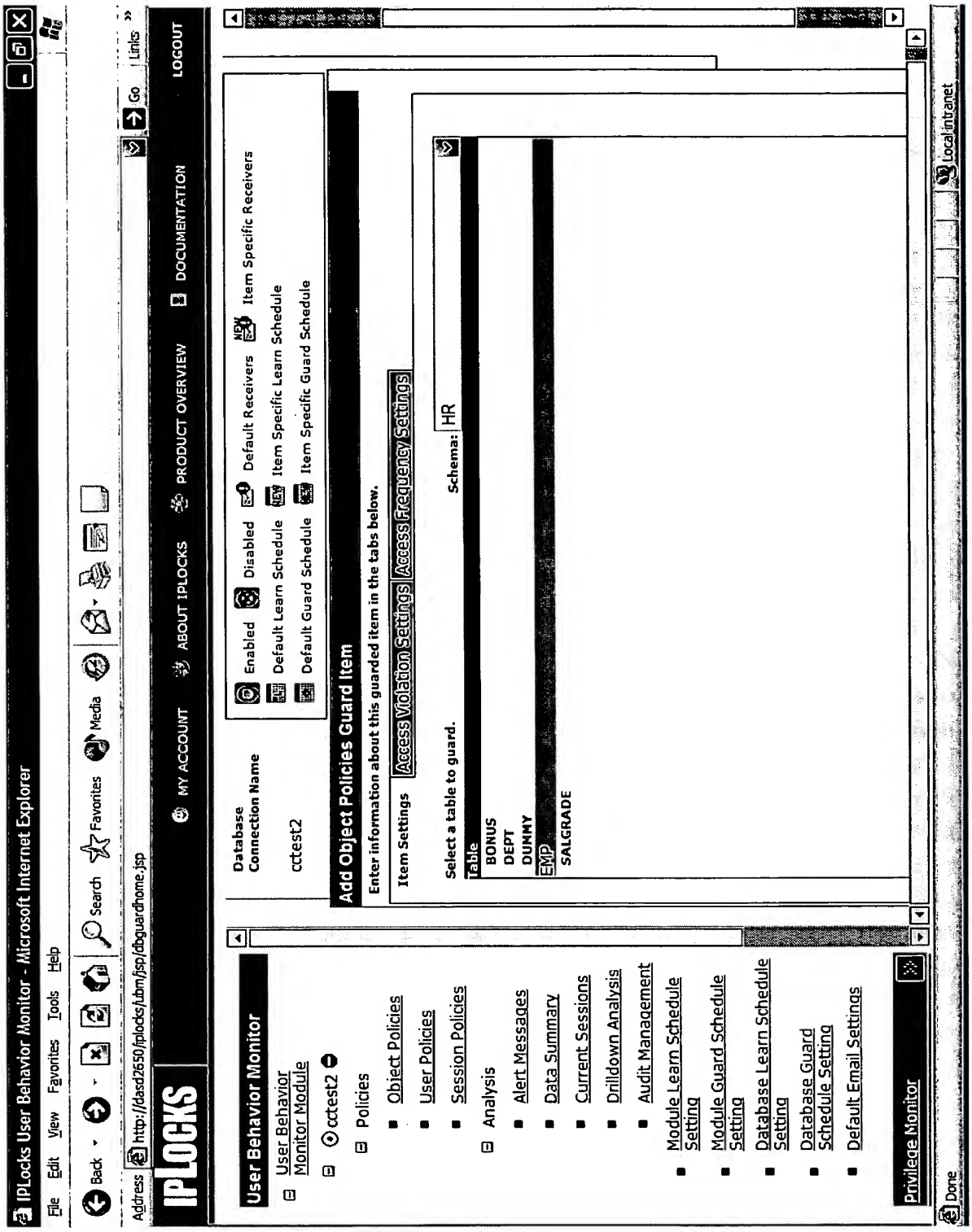
IPLocks User Behavior Monitor - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://dasd2650/iplocks/jtbm/jsp/dbguardhome.jsp
IPLOCKS
MY ACCOUNT
ABOUT IPLOCKS
PRODUCT OVERVIEW
DOCUMENTATION
LOGOUT
User Behavior Monitor
User Behavior Monitor Module
cctest2
Policies
Object Policies
User Policies
Session Policies
Analysis
Alert Messages
Data Summary
Current Sessions
Drilldown Analysis
Audit Management
Module Learn Schedule Setting
Module Guard Schedule Setting
Database Learn Schedule Setting
Database Guard Schedule Setting
Default Email Settings
Privilege Monitor
Database Connection Name
cctest2
Enabled
Disabled
Default Receivers
Item Specific Receivers
Default Learn Schedule
Item Specific Learn Schedule
Default Guard Schedule
Item Specific Guard Schedule
Add Object Policies Guard Item
Enter information about this guarded item in the tabs below.
Item Settings
Access Violation Settings
Access Frequency Settings
Select a table to guard.
Schema: HR
Table
BONUS
DEPT
DUMMY
EMP
SALGRADE
Done
Local intranet

FIG 6E

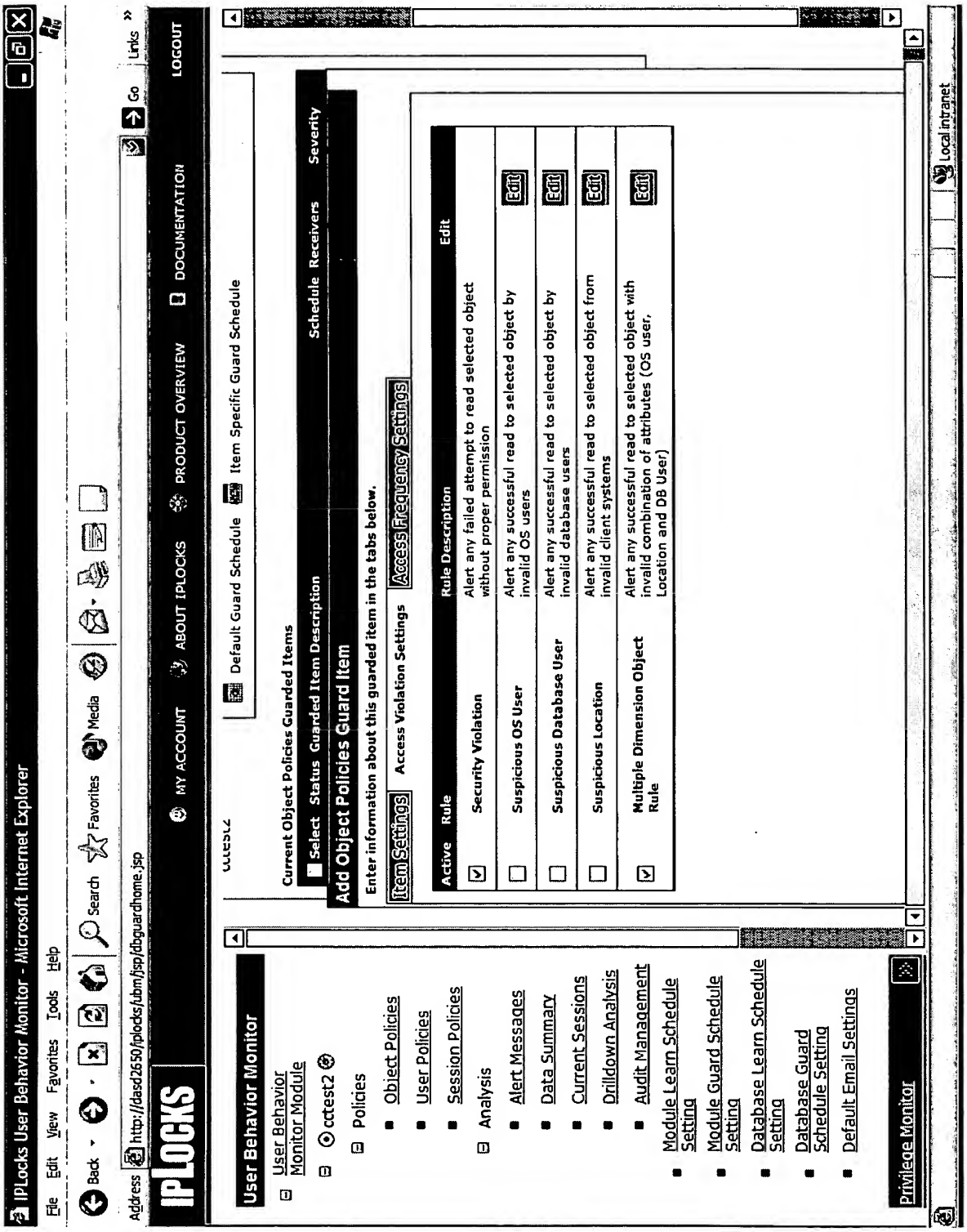
IPLocks User Behavior Monitor - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://dasd2650/iplocks/ubm/jsp/dbguardhome.jsp
IPLOCKS
MY ACCOUNT
ABOUT IPLOCKS
PRODUCT OVERVIEW
DOCUMENTATION
LOGOUT
User Behavior Monitor
User Behavior Monitor Module
cctest2
Policies
Object Policies
User Policies
Session Policies
Analysis
Alert Messages
Data Summary
Current Sessions
Drilldown Analysis
Audit Management
Module Learn Schedule Setting
Module Guard Schedule Setting
Database Learn Schedule Setting
Database Guard Schedule Setting
Default Email Settings
Privilege Monitor
Default Guard Schedule
Item Specific Guard Schedule
Current Object Policies Guarded Items
Select Status Guarded Item Description Schedule Receivers Severity
Add Object Policies Guard Item
Enter information about this guarded item in the tabs below.
Item Settings
Access Violation Settings
Access Frequency Settings
Active Rule Rule Description Edit
Security Violation Alert any failed attempt to read selected object without proper permission
Suspicious OS User Alert any successful read to selected object by invalid OS users Edit
Suspicious Database User Alert any successful read to selected object by invalid database users Edit
Suspicious Location Alert any successful read to selected object from invalid client systems Edit
Multiple Dimension Object Rule Alert any successful read to selected object with invalid combination of attributes (OS user, Location and DB User) Edit
Local intranet

FIG 6F

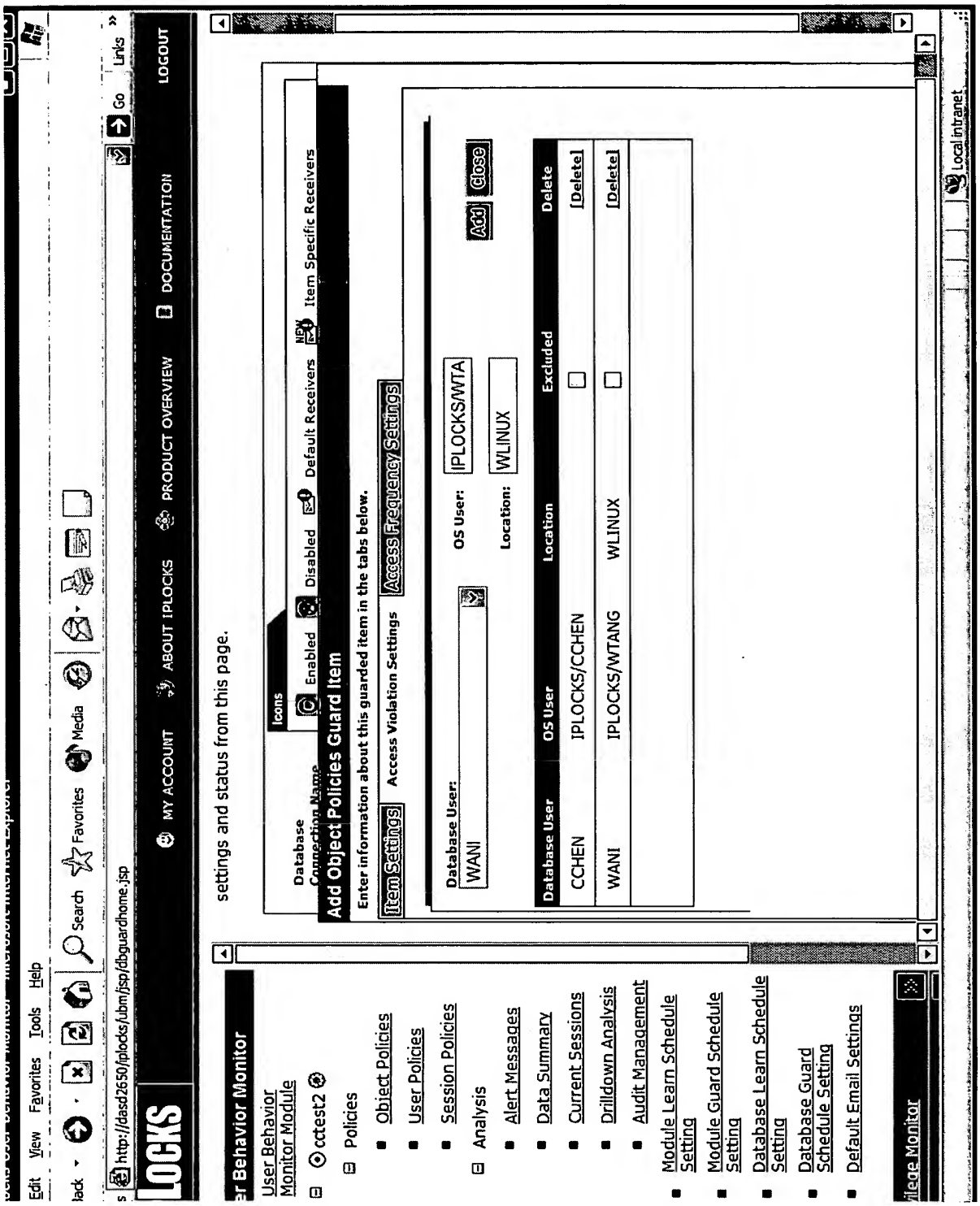
Edit View Favorites Tools Help
Search Favorites Media
http://dasd2650/iplocks/ubm/jsp/dbguardhome.jsp
LOCKS
MY ACCOUNT
ABOUT IPLOCKS
PRODUCT OVERVIEW
DOCUMENTATION
LOGOUT
User Behavior Monitor Module
cctest2
Policies
Object Policies
User Policies
Session Policies
Analysis
Alert Messages
Data Summary
Current Sessions
Drilldown Analysis
Audit Management
Module Learn Schedule Setting
Module Guard Schedule Setting
Database Learn Schedule Setting
Database Guard Schedule Setting
Default Email Settings
settings and status from this page.
Database Connection Name
Icons
Enabled
Disabled
Default Receivers
Item Specific Receivers
Add Object Policies Guard Item
Enter information about this guarded item in the tabs below.
Item Settings
Access Violation Settings
Access Frequency Settings
Database User:
WANI
OS User:
IPLOCKS/WTA
Location:
WLINUX
Add
Close
Database User
OS User
Location
Excluded
Delete
CCHEN
IPLOCKS/CCHEN
[Deletel
WANI
IPLOCKS/WTANG
WLINUX
[Deletel
Local intranet

FIG 6G

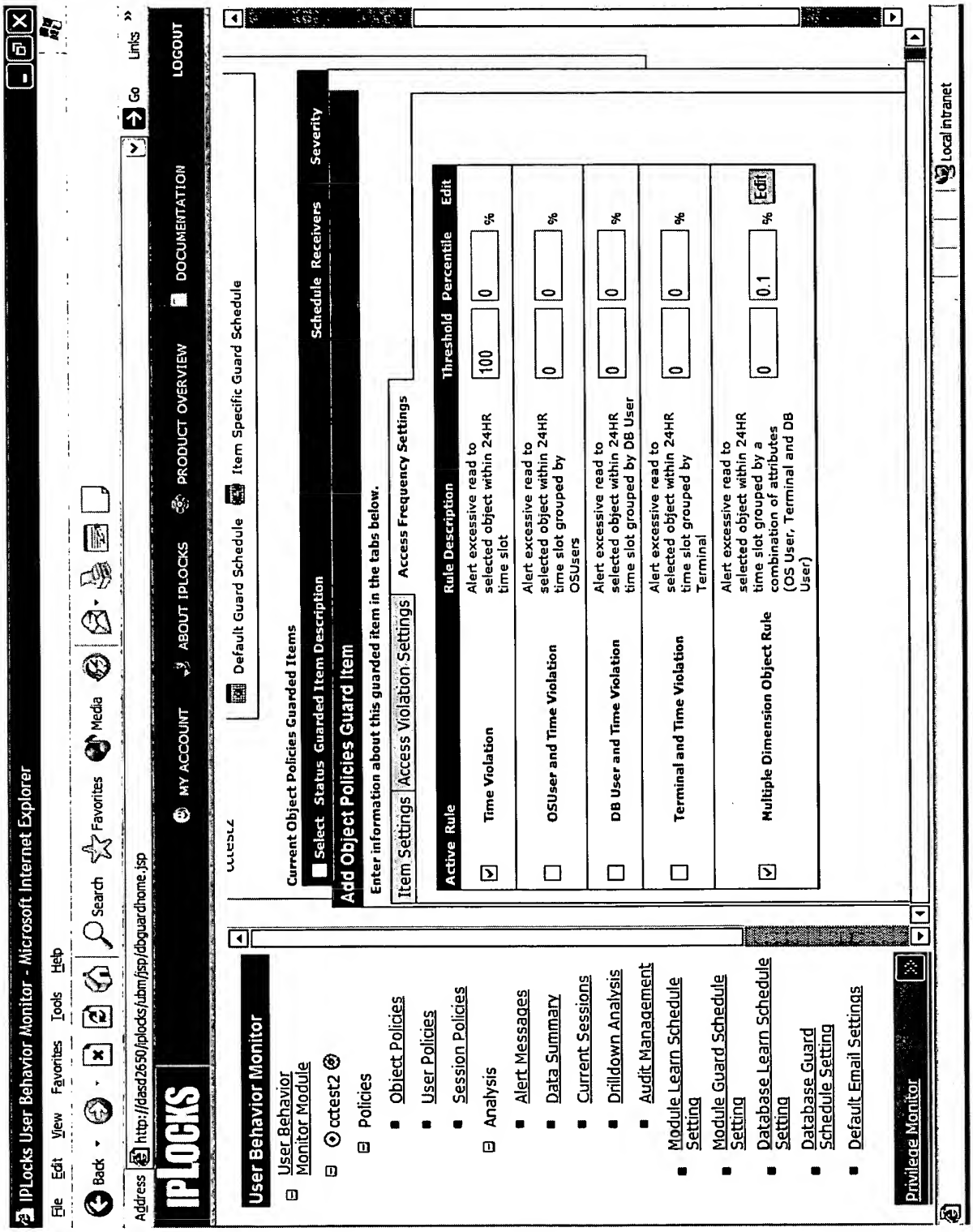
IPLocks User Behavior Monitor - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://dasd2650/iplocks/ubm/jsp/dbguardhome.jsp
IPLOCKS
MY ACCOUNT
ABOUT IPLOCKS
PRODUCT OVERVIEW
DOCUMENTATION
LOGOUT
User Behavior Monitor
User Behavior Monitor Module
cctest2
Policies
Object Policies
User Policies
Session Policies
Analysis
Alert Messages
Data Summary
Current Sessions
Drilldown Analysis
Audit Management
Module Learn Schedule Setting
Module Guard Schedule Setting
Database Learn Schedule Setting
Database Guard Schedule Setting
Default Email Settings
Privilege Monitor
Default Guard Schedule
Item Specific Guard Schedule
Current Object Policies Guarded Items
Select Status Guarded Item Description Schedule Receivers Severity
Add Object Policies Guard Item
Enter information about this guarded item in the tabs below.
Item Settings
Access Violation Settings
Access Frequency Settings
Active Rule
Rule Description
Threshold
Percentile
Edit
Time Violation
Alert excessive read to selected object within 24HR time slot
100
0
%
OSUser and Time Violation
Alert excessive read to selected object within 24HR time slot grouped by OSUsers
0
0
%
DB User and Time Violation
Alert excessive read to selected object within 24HR time slot grouped by DB User
0
0
%
Terminal and Time Violation
Alert excessive read to selected object within 24HR time slot grouped by Terminal
0
0
%
Multiple Dimension Object Rule
Alert excessive read to selected object within 24HR time slot grouped by a combination of attributes (OS User, Terminal and DB User)
0
0.1
%
Edit
Local intranet

FIG 6H

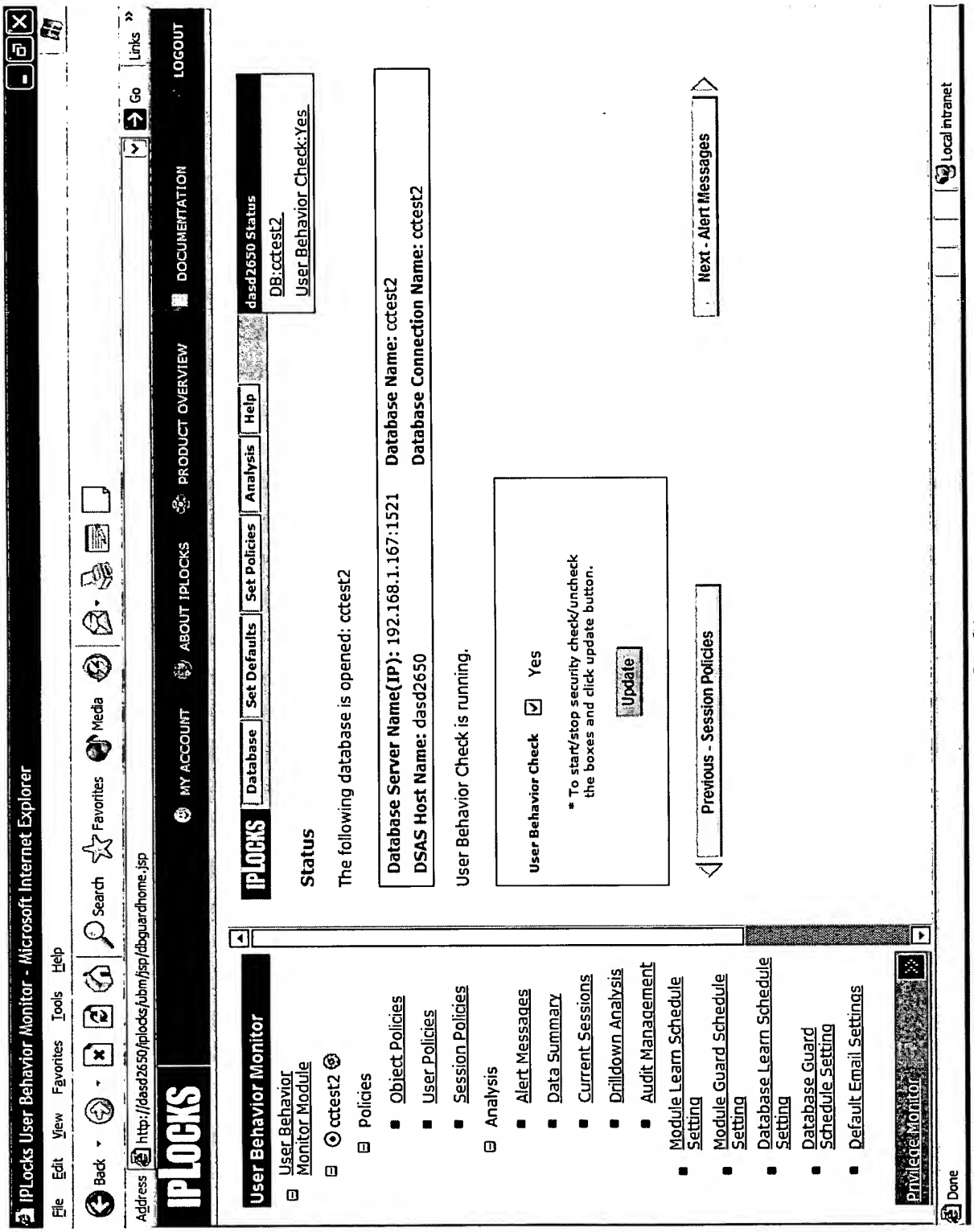
IPLocks User Behavior Monitor - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://dasd2650/iplocks/ubm/jsp/dbguardhome.jsp
Go Links
IPLOCKS
MY ACCOUNT
ABOUT IPLOCKS
PRODUCT OVERVIEW
DOCUMENTATION
LOGOUT
User Behavior Monitor
User Behavior Monitor Module
cctest2
Policies
Object Policies
User Policies
Session Policies
Analysis
Alert Messages
Data Summary
Current Sessions
Drilldown Analysis
Audit Management
Module Learn Schedule Setting
Module Guard Schedule Setting
Database Learn Schedule Setting
Database Guard Schedule Setting
Default Email Settings
Privilege Monitor
IPLOCKS
Database
Set Defaults
Set Policies
Analysis
Help
dasd2650 Status
DB:cctest2
User Behavior Check:Yes
Status
The following database is opened: cctest2
Database Server Name(IP): 192.168.1.167:1521
DSAS Host Name: dasd2650
Database Name: cctest2
Database Connection Name: cctest2
User Behavior Check is running.
User Behavior Check
Yes
* To start/stop security check/uncheck the boxes and click update button.
Update
Previous - Session Policies
Next - Alert Messages
Done
Local intranet

FIG 6I

cautionary UBM alert raised from cctest2 (Object Policies:HR.EMP) - Message (HTML) - Unicode (UTF-8)

File Edit View Insert Format Tools Actions Help

Reply | Reply to All | Forward

From: dssadmin@iplocks.com
To: Wani Tang
Cc:
Subject: cautionary UBM alert raised from cctest2 (Object Policies:HR.EMP)

Sent: Fri 1/23/2004 2:11 PM

Brief Description:
Alarm ID: 1,782
Severity: cautionary
Violated Policy: Object Policies
Guarded Item: HR.EMP
Alarm Generated Time: 2004-01-23 14:24:22
Application: UBM@dasd2650:80
Database: CCTEST2@192.168.1.166:1521
Detailed Description:
Database object HR.EMP is accessed by DB user WANI at 1/23/04 2:11 PM with suspicious attribute combination:
Terminal=CKDESKTOP, OS User=IPLOCKS\CKCHOU and DB User=WANI

To update alarm status use the link:Update Status

FIG 6J

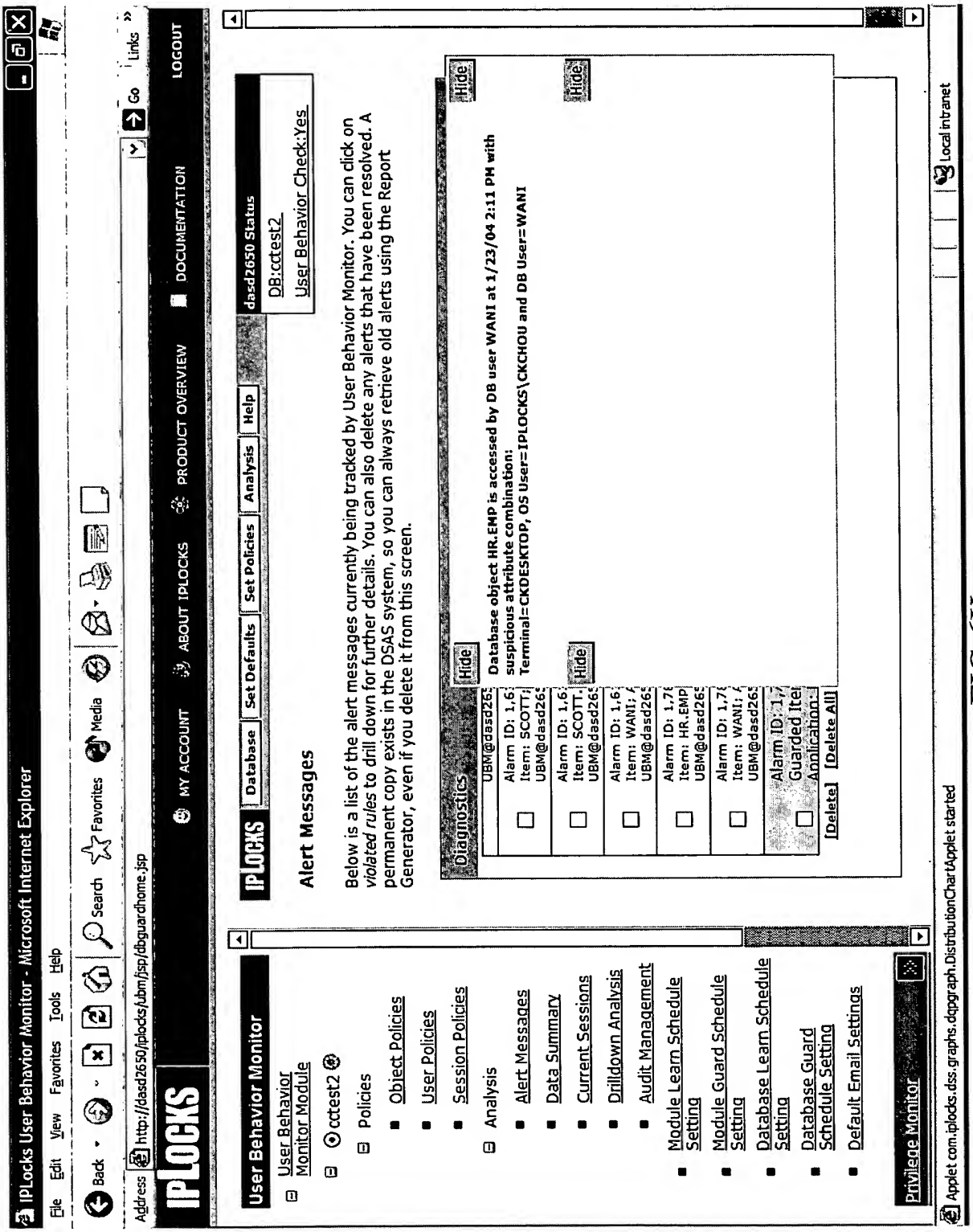
IPLocks User Behavior Monitor - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://dasd2650/iplocks/ubm/jsp/dbguardhome.jsp
IPLOCKS
MY ACCOUNT
ABOUT IPLOCKS
PRODUCT OVERVIEW
DOCUMENTATION
LOGOUT
User Behavior Monitor
User Behavior Monitor Module
cctest2
Policies
Object Policies
User Policies
Session Policies
Analysis
Alert Messages
Data Summary
Current Sessions
Drilldown Analysis
Audit Management
Module Learn Schedule Setting
Module Guard Schedule Setting
Database Learn Schedule Setting
Database Guard Schedule Setting
Default Email Settings
Privilege Monitor
IPLOCKS
Database
Set Defaults
Set Policies
Analysis
Help
dasd2650 Status
DB:cctest2
User Behavior Check:Yes
Alert Messages
Below is a list of the alert messages currently being tracked by User Behavior Monitor. You can click on violated rules to drill down for further details. You can also delete any alerts that have been resolved. A permanent copy exists in the DSAS system, so you can always retrieve old alerts using the Report Generator, even if you delete it from this screen.
Diagnostics
Hide
Database object HR.EMP is accessed by DB user WANI at 1/23/04 2:11 PM with suspicious attribute combination:
Terminal=CKDESKTOP, OS User=IPLOCKS\CKCHOU and DB User=WANI
[Delete] [Delete All]
Applet com.iplocks.dss.graphs.dqpgraph.DistributionChartApplet started
Local intranet

FIG 6K

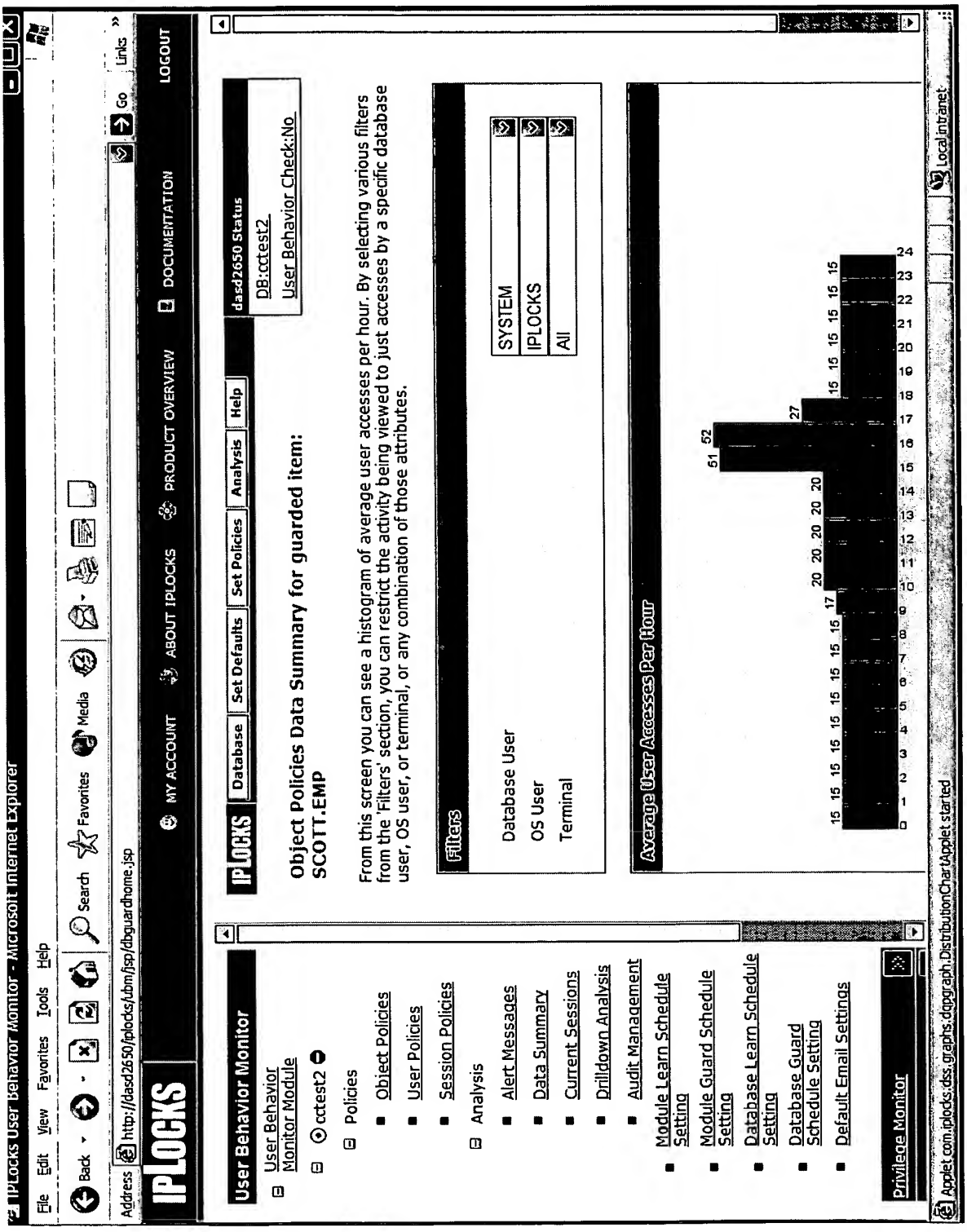
IPLOCKS User Behavior Monitor - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://dasd2650/iplocks/Ubm/jsp/dbguardhome.jsp
IPLOCKS
MY ACCOUNT
ABOUT IPLOCKS
PRODUCT OVERVIEW
DOCUMENTATION
LOGOUT
User Behavior Monitor
User Behavior Monitor Module
cctest2
Policies
Object Policies
User Policies
Session Policies
Analysis
Alert Messages
Data Summary
Current Sessions
Drilldown Analysis
Audit Management
Module Learn Schedule Setting
Module Guard Schedule Setting
Database Learn Schedule Setting
Database Guard Schedule Setting
Default Email Settings
Privilege Monitor
Database
Set Defaults
Set Policies
Analysis
Help
dasd2650 Status
DB:cctest2
User Behavior Check:No
Object Policies Data Summary for guarded item:
SCOTT.EMP
From this screen you can see a histogram of average user accesses per hour. By selecting various filters from the 'Filters' section, you can restrict the activity being viewed to just accesses by a specific database user, OS user, or terminal, or any combination of those attributes.
Filters
Database User
OS User
Terminal
SYSTEM
IPLOCKS
All
Average User Accesses Per Hour
Applet com.iplocks.dss.graphs.dqpgraph.DistributionChartApplet started
Local intranet

FIG 6L

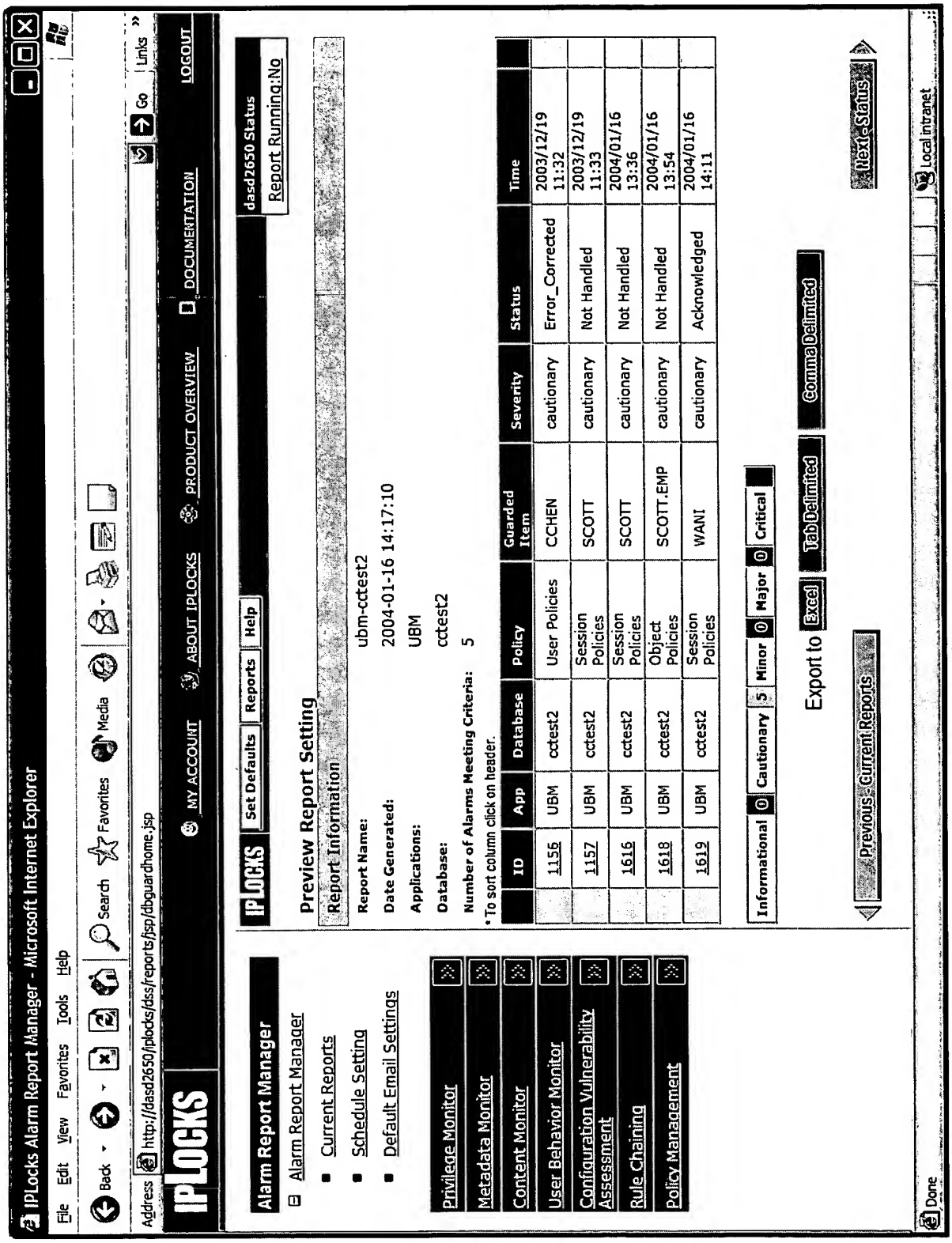
IPLocks Alarm Report Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://dasd2650/iplocks/dss/reports/jsp/dbguardhome.jsp
Go Links
IPLOCKS
MY ACCOUNT
ABOUT IPLOCKS
PRODUCT OVERVIEW
DOCUMENTATION
LOGOUT
Alarm Report Manager
Alarm Report Manager
Current Reports
Schedule Setting
Default Email Settings
Privilege Monitor
Metadata Monitor
Content Monitor
User Behavior Monitor
Configuration Vulnerability Assessment
Rule Chaining
Policy Management
IPLOCKS
Set Defaults
Reports
Help
dasd2650 Status
Report Running:No
Preview Report Setting
Report Information
Report Name: ubm-cctest2
Date Generated: 2004-01-16 14:17:10
Applications: UBM
Database: cctest2
Number of Alarms Meeting Criteria: 5
* To sort column click on header.
ID App Database Policy Guarded Item Severity Status Time
1156 UBM cctest2 User Policies CCHEN cautionary Error_Corrected 2003/12/19 11:32
1157 UBM cctest2 Session Policies SCOTT cautionary Not Handled 2003/12/19 11:33
1616 UBM cctest2 Session Policies SCOTT cautionary Not Handled 2004/01/16 13:36
1618 UBM cctest2 Object Policies SCOTT.EMP cautionary Not Handled 2004/01/16 13:54
1619 UBM cctest2 Session Policies WANI cautionary Acknowledged 2004/01/16 14:11
Informational 0 Cautionary 5 Minor 0 Major 0 Critical
Export to Excel Tab Delimited Comma Delimited
Previous Current Reports
Next Status
Done
Local intranet

FIG 6M

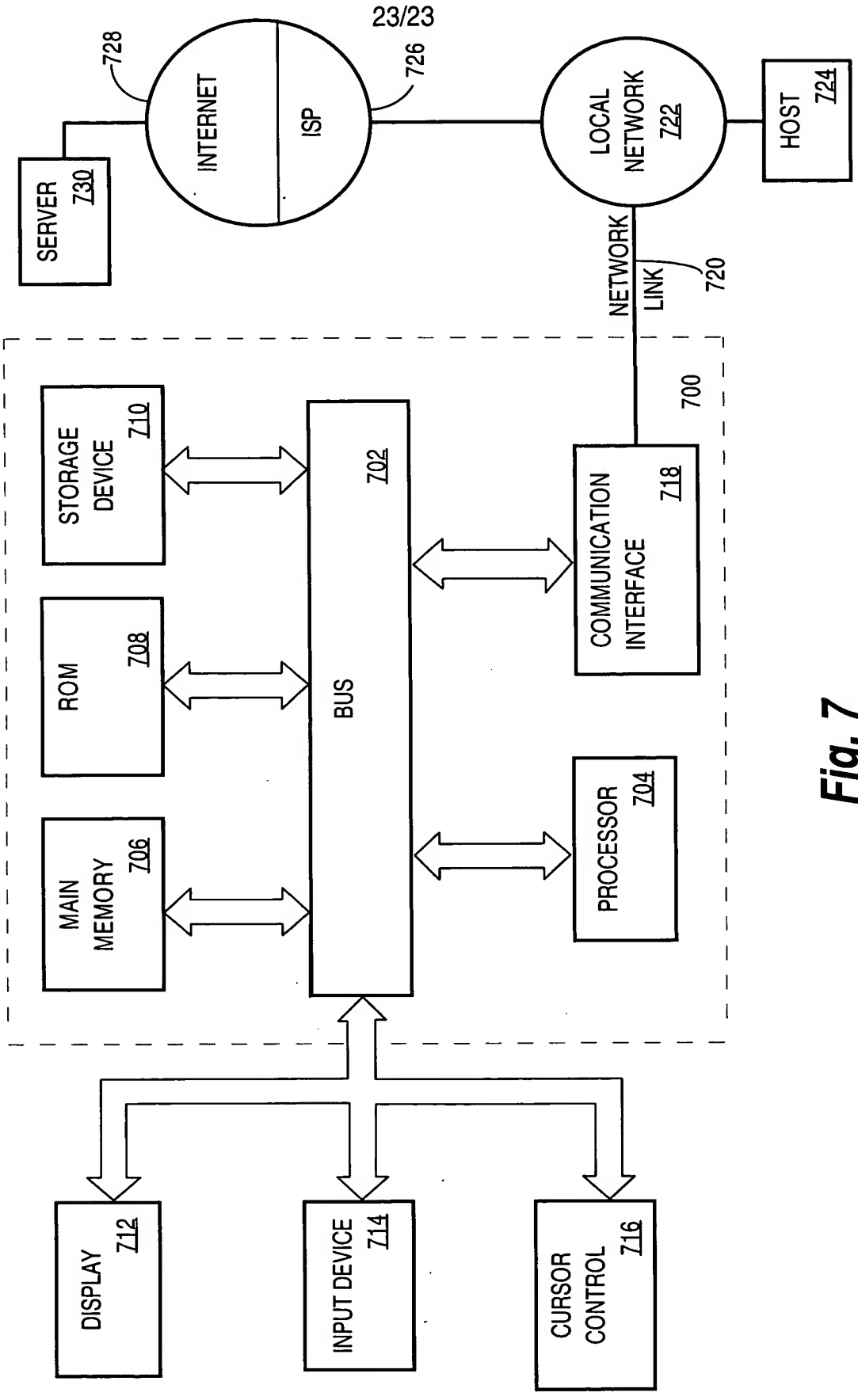
728
INTERNET
ISP
726
LOCAL NETWORK 722
HOST 724
SERVER 730
NETWORK LINK 720
700
STORAGE DEVICE 710
BUS 702
COMMUNICATION INTERFACE 718
ROM 708
MAIN MEMORY 706
PROCESSOR 704
DISPLAY 712
INPUT DEVICE 714
CURSOR CONTROL 716

Fig. 7